## REMARKS/ARGUMENTS

Claims 1-45 stand in the present application. Reconsideration and favorable action is respectfully requested in view of the following remarks.

In the Office Action, the Examiner has rejected claims 1-16 and 21-45 under 35 U.S.C. § 102(b) as being anticipated by Dondeti et al. ("Dondeti"), and has rejected claims 17-20 under 35 U.S.C. § 103(a) as being unpatentable over Dondeti. Applicant respectfully traverses the Examiner's §§ 102 and 103 rejections of the claims.

The Examiner's rejection of the claims based on Dondeti is misplaced in that Dondeti fails to teach or suggest several limitations of the present claims. More particularly, Dondeti simply does not teach or suggest the use of an "offset" as required by the present claims. For example, claim 1 requires:

> determining an offset for generating the updated first key of each node in the branch from a key of a previous node in the branch; and
>
> broadcasting each of said offsets in an unencrypted form so that, given the updated first key associated with the first node of said branch, each updated first key of said branch of nodes can be calculated. (emphasis supplied)

An "offset" is clearly defined in the present application at Figure 4 and page 12, lines 23 onwards. As explained in the present application, an offset message can be thought of in terms of the distance, or value difference, between two chains of keys. A first chain is generated from the key X0, and a second chain generated from Y0. Both chains are formed by applying the one-way function (f), so that "the user knowing the root key Y0 of chain Y can, given the correct offset message, recover X2" (page 13 lines 23 and 24). As graphically shown in Figure 4, it is possible to "move" from Y1 to obtain X2 if

the offset value is supplied. The offset is calculated by the central key server, since only the server has knowledge of the distance between the two chains.

A secure version of this method of moving from one value to another is shown in Figure 5, wherein an intermediate key is used temporarily and only to allow generation of e.g. X2 from Y1 (page 14 lines 4 to 31). In a tree structure implementation such as that shown in Figure 6, two nodes in a keypath e.g. K1 and K12, may be said to correspond to Y1 and X2 of Figure 5, in that they are part of two unrelated one-way function chains: page 17 lines 24 to 31.

Thus if the value of node K1 is "10" and the offset value is "5", it is then possible to "move" to node 12 which has a value of "15". These values are of course crude and inaccurate as the offset is a binary number and moreover is mixed using, e.g., an XOR function before the move from K1 to K12 is complete - and so are purely to assist understanding.

An offset message which relates to a specific key (e.g. Offset_m1 relates to key K_m1) is broadcast by the central key server to the entire group: page 19 lines 3 to 12. Because only the member of the group having knowledge of the key K_m1 can use the particular offset message Offset_m1, the offset message may be transmitted in plaintext or otherwise without need for encryption. This is a significant advantage over prior art methods which reduces the amount of bandwidth and computation required, especially at the member end.

In Dondeti, as in the subject invention, keys are updated upon a join event. Instead of the system broadcasting offset values in an unencrypted format however, Dondeti provides that key updating is carried out by the sending of various blinded and

unblinded keys which are freshly generated. See Dondeti at column 5, lines 51-64. Significantly, all keys need to be encrypted for transmission. See Dondeti at column 5, lines 64 and 65. Thus it is not possible in the Dondeti method to broadcast the equivalent of Applicant's offset (which is used to generate the updated keys) in an unencrypted form, as required by, e.g., claim 1.

The Examiner alleges that the binary ID of Dondeti corresponds to the required offset, but this is plainly wrong as the binary ID does nothing more than identify a member (22) to define key associations groups (22a). See Dondeti at column 3, lines 30 and 31. These groups are stated in Dondeti (column 2, lines 44 and 45) as merely a group composed of a number of members.

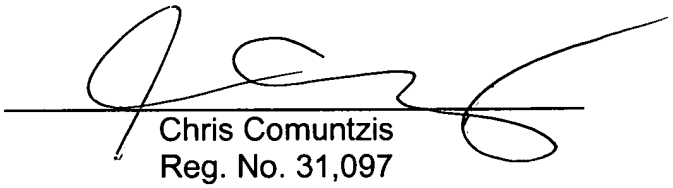
Dondeti simply does not in any way teach or suggest the use of anything similar to the offset value required by the present claims in the generation of key updates in a key distribution system, let alone that the offsets are broadcast in an unencrypted form. Thus, Dondeti fails to teach or suggest the above noted limitations of independent claim 1 and similar limitations in independent claim 22. Accordingly, independent claims 1 and 22 and their respective dependent claims are not anticipated by or obvious in view of Dondeti.

With respect to independent claim 38, as noted previously, Dondeti does not teach or suggest that an encryption key includes "a join field and a leave field." The portions of Dondeti cited by the Examiner simply do not contain this teaching. Accordingly, independent claim 38 and its respective dependent claims are also not anticipated by Dondeti.

Therefore, in view of the above remarks, it is respectfully requested that the application be reconsidered and that all of claims 1-45, standing in the application, be allowed and that the case be passed to issue. If there are any other issues remaining which the Examiner believes could be resolved through either a supplemental response or an Examiner's amendment, the Examiner is respectfully requested to contact the undersigned at the local telephone exchange indicated below.

Respectfully submitted,

**NIXON & VANDERHYE P.C.**

By: 

Chris Comuntzis
Reg. No. 31,097

CC:lmr
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100